UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,240	06/26/2001	Zheng Qi	BRCMP013A	3459

7590 12/30/2005

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 12/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,240	QI ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-20 and 22-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-20 and 22-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/18/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/18/2005 has been entered.

Claims 1-6, 8-20, and 22-28 are pending.

Information Disclosure Statement

Applicant's IDS submitted on 10/18/2005 has been considered.

Response to Amendment

Applicant's amendments filed 8/29/2005 has been considered. Please note new rejections below.

Response to Arguments

Applicant's arguments filed 8/29/2005 have been fully considered but they are not persuasive. Applicant argues that the prior arts of record does not teach "the second multiplexer receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing." The examiner respectfully disagrees.

The two-level multiplexer recited in the independent claims were as applicant noted, rejected under Windirsch. The examiner submits that Windirsch also discloses the above-recited limitation that applicant argues is not met by the art of record. As a

preliminary matter, the examiner first directs applicant to review pages 173-175 of Mano for an explanation of what a multiplexer is and how it works. The explanation provided by Mano will be useful in understanding how Windirsch meets the above-recited limitation. Basically, Mano defines a multiplexer as a circuit that selects binary information from one of its many input lines and directs that information to a single output line, where the selection is controlled by a set of selection lines (p173, section 5-6, paragraph 1).

Windirsch defines an encryption/decryption round as r*p clock pulses, where r represents the number of rounds required by the encryption algorithm, i.e. the passage of data items to be processed through module 3, and p represents the number of pipeline stages (col 6, lines 39-45). Note in Figure 1 that feedback signal R is derived from a shift/concatenation done using the output from module 43. Module 43 in turn gets an input from the encryption/decryption pipeline. One sees from the figure and from the definition provided by Windirsch on column 6, lines 39-45 of what a cryptographic round is that R could not have been obtained unless a round of cryptographic processing had been achieved, thus R is feedback data from a previous round of cryptographic processing. In column 4, lines 42-60, Windirsch discloses R is fed back into multiplexer 23, i.e. second multiplexer, as a third input signal. When signal R is fed back into the multiplexers seen in Figure 1, one sees that it is but one input into the multiplexers that it is fed into. Examining multiplexer 23, for example, one sees that the multiplexer has as its inputs: signal R, the output from multiplexer 9, and the output from register 1, which is start values 21. Though Windirsch does not

explicitly disclose a second signal, one sees that there is but one output from multiplexer 23 and from Mano's explanation of how a multiplexer works, one of ordinary skill can understand that a signal to select one of the inputs of multiplexer 23 as the output of the multiplexer is inherent to multiplexer 23 or to any multiplexer. This signal reads on the second signal which causes the multiplexer to select/associate R with the second position, i.e. the output of the multiplexer. From examining Figure 1, one can safely assume that should R be associated with the second position that R will be used in at least part of the next round of cryptographic processing.

The examiner believes that the above teachings by Windirsch, especially in light of what one of ordinary skill knows about how a multiplexer works, renders the amendments by applicant obvious to the current art of record. For the purpose of fostering good relations with the public, the examiner will not make this office action final immediately following the filing of the RCE so that applicant may have another chance to amend the current set of claims to recite or more clearly define limitations that might be allowable over art.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-6, 8-20, and 22-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. As per claims 1 and 15, the examiner submits that applicant is incorrectly using commas in several places, which renders the claim unclear and indefinite. Particularly, the limitation ", and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing" makes no sense. The examiner suspects applicant may have unintentionally added commas where there should not be any commas. Consider instead the following: "and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing with the second position for a next round of cryptographic processing."
2. Claims 2 and 16 recites "the portion" on line 3, which lacks antecedent basis. It is unclear if applicant meant the first portion, the second portion, or some other portion.
3. Claims 4 and 18 recite in line 2, "the multiplexer", which lacks antecedent basis. The examiner believes applicant meant "the two-level multiplexer".
4. Any claims not specifically addressed are rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 8-20, and 22-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (US 6,769,063) in view of Windirsch (US 6,760,439) and further in view of Callum (US 6,320,964).

Claims 1 and 15:

Kanda discloses a cryptographic engine as per claim 1 for performing cryptographic operations on a data block (col 1, lines 8-15). Kanda also discloses an integrated circuit layout associated with a cryptography engine as per claim 15 for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine (col 1, lines 8-15). Kanda further discloses the cryptographic engine and the integrated circuit layout comprising:

1. A key scheduler configured to provide keys for cryptographic operations (col 7, lines 11-25).
2. Expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a first portion of the data block occupying the first position (col 15, lines 8-20 and Figure 8A-8D).
3. Permutation logic configured to alter a second bit sequence corresponding to the first portion of the data block (col 1, lines 31-46).

Kanda does not explicitly disclose:

1. A two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level.
2. Permutation logic coupled to the expansion logic.
3. Wherein the multiplexer on the first level selects initial input data responsive to a first signal, and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing.

However, Windirsch discloses a two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level (col 1, lines 35-47). Windirsch discloses the limitation, wherein the multiplexer on the first level selects initial input data responsive to a first signal (col 3, lines 49-63), and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing (Fig 1; col 4, lines 42-60; and col 6, lines 39-45). Further, Callum discloses permutation logic coupled to the expansion logic (Figure 3, items 319 and 320).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have incorporated Windirsch and Callum's teachings with Kanda's according to the limitations recited in claims 1 and 15. One of ordinary skill would have been motivate to incorporate Windirsch's teachings

because he discloses that it would allow for a single device that can be operated in different ISO-10116 standard modes (col 1, lines 35-67 and col 2, 1st paragraph) and allow for simultaneous processing of a number of data streams (col 2, lines 12-16). One of ordinary skill would have been motivated to incorporate Callum's teachings because he discloses that his teachings would allow a cryptography engine to better handle instruction-intensive bit permutation and thereby achieve greater cryptography speed (abstract).

Claims 2 and 16:

Kanda further discloses the cryptographic engine, further comprising an Sbox configuration to alter a third bit sequence corresponding to the portion of the data block by compacting a size of the third bit sequence and altering the third bit sequence using Sbox logic (col 3, lines 31-52; col 10, last paragraph; and col 11, 1st paragraph).

Claims 3 and 17:

Kanda further discloses the cryptography engine, wherein the cryptography engine is a DES engine (col 14, lines 15-28).

Claims 4 and 18:

Windirsch further discloses two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level (Fig 1, items 13, 25, 29, and 33). The motivations for combining the teachings of Kanda, Windirsch, and Callum are the same as for claims 1 and 15

Claims 5 and 19:

Kanda further discloses the cryptography engine, wherein the first bit sequence is less than 32 bits (col 2, lines 1-21).

Claims 6 and 20:

Kanda further discloses the cryptography engine, wherein the first bit sequence is four bits (col 17, lines 9-28).

Claims 8 and 22:

Callum further teaches the cryptography engine, wherein the expansion logic and the permutation logic are associated with DES operations (col 3, lines 32-47 and Fig 3, items 319 and 320). The motivations for combining the teachings of Kanda, Windirsch, and Callum are the same as for claims 1 and 15.

Claims 9 and 23:

Windirsch further teaches pipelining being used in an encryption/decryption device (col 2, lines 12-35). One of ordinary skill would be motivated to incorporate Windirsch's teachings of pipelining into the combination system of Kanda, Windirsch, and Callum for the same reasons as for claims 1 and 15.

Claims 10 and 24:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a plurality of stages (col 1, lines 18-67).

Claims 11 and 25:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a determination stage (col 15, lines 21-33).

Claims 12 and 26:

Callum further discloses the cryptography engine, wherein the key scheduler comprises a shift stage (col 4, lines 46-67 and col 5, lines 1-5). The motivations for combining the teachings of Kanda, Windirsch, and Callum are the same as for claims 1 and 15.

Claims 13 and 27:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a propagation stage (col 2, lines 1-21).

Claims 14 and 28:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a consumption stage (col 3, lines 30-51).

Claims 4 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (US 6,769,063) in view of Windirsch (US 6,760,439) and further in view of Callum (US 6,320,964) and Steinman et al (US 6,591,349).

Claims 4 and 18:

Kanda does not explicitly teach two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on a second level. However, Steinman teaches 2-to-1 multiplexer usage (col 3, last paragraph and col 4, 1st paragraph). It would have been obvious to one of ordinary skill at the time the applicant's invention was made to employ Steinman's teachings within the combination system of Kanda, Windirsch, and Callum

as it would allow increased performance of a computer memory system by reducing lost clock cycles (Steinman's abstract). It would have been obvious to one of ordinary skill to have two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level because it would allow for increased performance of DES or triple DES engine as the performance of the computer improved in using 2-to-1 multiplexers. The speed up in clock cycle improves the performance of DES.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich

Examiner
Art Unit 2135

PP